- **Exact replica of production systems**
- Applications and software are constantly updated
- Flip a switch and everyting moves
- **It take hours to bring online**
- Real-time synchronization
- Almost all data ready to go - often just a quick update
- Very expensive

Penetration Test - Basics

This topic will be covered with details in Chapter 14 - Pentesting.

A penetration test, colloquially known as a pen test, pentest or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.

⚠️ **Not to be confused with a vulnerability assessment.**

- Clearly defined, full scale test of security controls
- Phases
    - **Preparation** - Contracts and team determined
    - **Assessment** - All hacking phases (reconnaissance, scanning, attacks, etc.)
    - **Post-Assessment** - Reports & conclusions
- Types
    - **Black Box** - Done without any knowledge of the system or network.
    - **White Box** - When the attacker have complete knowledge of the system provided by the owner/target.
    - **Gray Box** - When the attacker has some knowledge of the system and/or network

Law Categories

- **Criminal** - Laws that protect public safety and usually have jail time attached.
- **Civil** - Private rights and remedies.
- **Common** - Laws that are based on societal customs.

Laws and Standards:

OSSTM Compliance

"Open Source Security Testing Methodology Manual" maintained by ISECOM , defines three types of compliance.

- **Legislative** - Deals with government regulations (Such as SOX and HIPAA).
- **Contractual** - Deals with industry / group requirement (Such as PCI DSS).
- **Standards based** - Deals with practices that must be followed by members of a given group/organization (Such as ITIL ,ISO and OSSTMM itself).
- **OSSTM Controls**
    - **OSSTM Class A - Interactive Controls**
        - *Authentication* - Provides for identification and authorization based on credentials.
        - *Indemnification* - Provided contractual protection against loss or damages.
        - *Subjugation* - Ensures that interactions occur according to processes defined by the asset owner.
        - *Continuity* - Maintains interactivity with assets if corruption of failure occurs.
        - *Resilience* - Protects assets from corruption and failure.
- **OSSTM Class B - Process Controls**
    - *Non-repudiation* - Prevents participants from denying its actions
    - *Confidentiality* - Ensures that only participants know of an asset
    - *Privacy* - Ensures that only participants have access to the asset
    - *Integrity* - Ensures that only participants know when assets and processes change
    - *Alarm* - Notifies participants when interactions occur

PCI-DSS

"Payment Card Industry Data Security Standard" Standard for organizations handling Credit Cards, ATM cards and other POS cards.

ISO 27001

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system.

ISO 27002 AND 17799

Based on BS799 but focuses on security objectives and provides security controls based on industry best practice.

HIPAA

"Health Insurance Portability and Accountability Act" a law that set's privacy standards to protect patient medical records and health information shared between doctors, hospitals and insurance providers.

SOX

"Sarbanes-Oxley Act" Law that requires publicly traded companies to submit to independent audits and to properly disclose financial information.

DMCA

"The Digital Millennium Copyright Act" is a 1998 United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization. It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works.

FISMA

"Federal Information Security Modernization Ac Of 2002" A law updated in 2004 to codify the authority of the Department of Homeland Security with regard to implementation of information security policies. *(For GOV. agencies)*

NIST-800-53

Catalogs security and privacy controls for federal information systems, created to help implementation of FISMA.

FITARA

"Federal Information Technology Acquisition Reform Act" A 2013 bill that was intended to change the framework that determines how the US GOV purchases technology.

COBIT

"Control Object for Information and Related Technology" IT Governance framework and toolset, created by ISACA and ITGI

GLBA

"U.S Gramm-Leach-Bliley Act" Law that protects the confidentiality and integrity of personal information that is collected by financial institutions.

CSIRT

"Computer Security Incident Response Team" CSIRT provided a single point of contact when reporting computer security incidents

ITIL

"Information Technology Infrastructure Library" - An operational framework developed in the '80s that standardizes IT management procedures

Essential Knowledge

OSI Model and TCP Model

- **The OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
- **The TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.

Layer	Device Type	OSI Layer	TCP/IP model	TCP/IP New (actual)	Protocols	PDU
7	Gateway	**Application**	Application	Application	HTTP, FTP, POP, SMTP, DNS, RIP	Data

Layer	Device Type	OSI Layer	TCP/IP model	TCP/IP New (actual)	Protocols	PDU
6	-	**Presentation**	Application	Application	HTTP, FTP, POP, SMTP, DNS, RIP, MIME	Data
5	-	**Session**	Application	Application	HTTP, FTP, POP, SMTP, DNS, RIP, SCP	Data
4	-	**Transport**	Transport	Transport	TCP/UDP	Segments
3	Router	**Network**	Internet	Network	IP, ARP, ICMP, IGMP	Packets
2	Switch/bridge	**Data Link**	Link	Data Link	Ethernet, Token Ring	Frames
1	Hubs/Repeater	**Physical**	Link	Physical	Ethernet, Token Ring	Bits

TCP Handshake

The Three-way handshake